Points of Finite Order on Elliptic Curves with Complex Multiplication

by

Loren D. Olson

Let E be an elliptic curve defined over $\mathbb{Q}$. The group of $\mathbb{Q}$-rational points of finite order on E is a finite group $T(E)$. In this article $T(E)$ is computed for all elliptic curves defined over $\mathbb{Q}$ admitting complex multiplication. First, it is shown that the only possible values for the order of $T(E)$ are $1,2,3,4$, or 6 for an elliptic curve E over $\mathbb{Q}$ with complex multiplication in $\mathbb{Q}(\sqrt{m})$, $m < 0$, m square-free. We then establish a number of results implying that certain of the values for the order of $T(E)$ are possible only for certain fields of complex multiplication, e.g. the order of $T(E)$ can be 4 only if $m = -1$. A standard form for an affine equation describing an elliptic curve with a given j-invariant is obtained and used to show that certain of these curves cannot have $\mathbb{Q}$-rational points of order 2, while others are forced to do so. We also give some necessary conditions on the j-invariant for E to have $\mathbb{Q}$-rational points of order 2. The remaining possibilities for the order of $T(E)$ are then considered. The results are summarized in the accompanying table.

In the final section we discuss the relationship of the results obtained here with the theory of anomalous primes for elliptic curves.

m	f	j	t
-1	1	$2^6 3^3$	2 or 4 (cyclic and non-cyclic)
-2	1	$2^6 5^3$	2
-3	1	0	1,2,3, or 6
-7	1	$-3^3 5^3$	2
-11	1	-2^{15}	1
-19	1	$-2^{15} 3^3$	1
-43	1	$-2^{18} 3^3 5^3$	1
-67	1	$-2^{15} 3^3 5^3 11^3$	1
-163	1	$-2^{18} 3^3 5^3 23^3 29^3$	1
-1	2	$2^3 3^3 11^3$	2 or 4 (cyclic)
-3	2	$2^4 3^3 5^3$	2 or 6
-7	2	$3^3 5^3 17^3$	2
-3	3	$-2^{15} 3^1 5^3$	1 or 3

§ 1. General results

Let E be an elliptic curve defined over $\mathbb{Q}$, i.e. a non-singular projective curve of genus one defined over $\mathbb{Q}$ together with a $\mathbb{Q}$-rational point e on E which acts as the identity element for the group law on E. Any such elliptic curve is isomorphic over $\mathbb{Q}$ to an elliptic curve defined by an affine equation of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1.1}$$

with $a_i \in \mathbb{Z}$. We define the following standard quantities with respect to the equation (1.1):

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta \end{aligned} \tag{1.2}$$

For the remainder of § 1, we assume that E admits complex multiplication in $\mathbb{Q}(\sqrt{m})$ with $m < 0$ a square-free integer. If A denotes the ring of integers in $\mathbb{Q}(\sqrt{m})$, then the endomorphism ring of E, $\mathrm{End}(E)$, is a subring of A of finite index and may be written as $\mathbb{Z} + fA$ for f a uniquely determined positive integer. f is called the <u>conductor</u> of $\mathrm{End}(E)$ in A. There are precisely 13 values in $\mathbb{Q}$ for the j-invariant of an elliptic curve E admit-

ting complex multiplication (cf. Serre [6,p.295]).

If D denotes the discriminant of $\mathbb{Q}(\sqrt{m})$ over $\mathbb{Q}$, then $D = m$ if $m \equiv 1 \pmod 4$ and $D = 4m$ if $m \not\equiv 1 \pmod 4$. Let $\left(\frac{a}{p}\right)$ denote the Legendre symbol of a with respect to a prime p. Recall that p splits in $\mathbb{Q}(\sqrt{m}) \iff \left(\frac{D}{p}\right) = 1 \iff \left(\frac{m}{p}\right) = 1$ and that p remains a prime in $\mathbb{Q}(\sqrt{m}) \iff \left(\frac{D}{p}\right) = -1 \iff \left(\frac{m}{p}\right) = -1$.

Let p be a prime where E has good reduction, and let N_p denote the number of $\mathbb{Z}/p\mathbb{Z}$ - rational points on the reduced curve. Let $f_p = 1 + p - N_p$ be the trace of the Frobenius. Let $\mathcal{P} = \mathcal{P}(E)$ be the set of all primes $p \geq 5$ such that E has good reduction at p. The following proposition is a well-known result (cf. Serre [7]).

Proposition 1.1. Let E be an elliptic curve defined over $\mathbb{Q}$ admitting complex multiplication. Let $p \in \mathcal{P}$. Then the following conditions are equivalent:

(1) $N_p = p + 1$

(2) $f_p = 0$

(3) p remains a prime in $\mathbb{Q}(\sqrt{m})$

(4) $\left(\frac{m}{p}\right) = -1$.

Let $\mathcal{P}_1 = \{p \in \mathcal{P} \mid \left(\frac{m}{p}\right) = -1\} = \{p \in \mathcal{P} \mid N_p = p+1\}$ and $\mathcal{P}_2 = \{p \in \mathcal{P} \mid \left(\frac{m}{p}\right) = 1\}$. Both $\mathcal{P}_1$ and $\mathcal{P}_2$ have density $1/2$ in $\mathcal{P}$.

Let $T(E)$ be the group of $\mathbb{Q}$-rational points on E which have finite order, and let t be the order of $T(E)$. Our purpose here is to determine t and $T(E)$ for all elliptic curves E defined over $\mathbb{Q}$ admitting complex multiplication. We will constantly make use of the following fact (cf. Tate [8,p.30]).

Proposition 1.2. Let E be any elliptic curve defined over $\mathbb{Q}$, and let $p \in$. Reduction modulo p induces a monomorphism from $T(E)$ into the group of $\mathbb{Z}/p\mathbb{Z}$-rational points on the reduced curve. Thus $t | N_p$ for all $p \in \mathcal{P}$.

Proposition 1.3. Let E be any elliptic curve defined over $\mathbb{Q}$ admitting complex multiplication. The only possible values for t are $1,2,3,4,$ or 6.

Proof: $t | N_p$ for all $p \in \mathcal{P}$. If $p \in \mathcal{P}_1$, then $N_p = p+1$, so that $t | (p+1)$, i.e. $p \equiv -1 \pmod{t}$. By Dirichlet's theorem the set of all $p \in \mathcal{P}$ such that $p \equiv -1 \pmod{t}$ has density $1/\phi(t)$ where ϕ is Euler's ϕ-function. If $\phi(t) \geq 3$, we have a contradiction. Thus $\phi(t) \leq 2$ and we must have $t \leq 6$ and $t \neq 5$.

Proposition 1.4. If $m \equiv 1 \pmod{4}$, then $t \neq 4$.

Proof: If $m \equiv 1 \pmod{4}$, then $-m \equiv 3 \pmod{4}$ and $-m$ is a prime greater than or equal to 3. Assume that $p \in \mathcal{P}$ is such that $p \equiv 1 \pmod{4}$. Then $\left(\frac{-1}{p}\right) = 1$.
We have $\left(\frac{m}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-m}{p}\right) = \left(\frac{-m}{p}\right) = \left(\frac{p}{-m}\right)$ by the quadratic reciprocity law. The arithmetic progression $(-4m)r + (-2m-1)$ contains infinitely many primes and hence there are infinitely many such in $\mathcal{P}$. Let $p = (-4m)r + (-2m-1)$ be one such. Computing modulo 4, we have $p \equiv (-4m)r + (-2m-1) \equiv -2m - 1 \equiv 1 \pmod{4}$. Computing modulo $-m$, we have $p \equiv (-4m)r + (-2m-1) \equiv -1 \pmod{-m}$. Thus $\left(\frac{m}{p}\right) = \left(\frac{p}{-m}\right) = \left(\frac{-1}{-m}\right) = -1$ since $-m \equiv 3 \pmod{4}$. Hence $p \in \mathcal{P}_1$ and so $N_p = p+1$. If $t = 4$, then $4 | (p+1)$ and so $p \equiv 3 \pmod{4}$, a contradiction.

Proposition 1.5. If $m = -2$, then $t \neq 4$.

Proof: There exist infinitely many primes p such that $p \equiv 5 \pmod 8$ and hence infinitely many such p in $\mathcal{P}$. Let p be one such in $\mathcal{P}$. Then $\left(\frac{-1}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = -1$. $\left(\frac{m}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{2}{p}\right) = -1$. Thus $p \in \mathcal{P}_1$ and so $N_p = p + 1$. If $t = 4$, then $4 \mid (p+1)$ and so $p \equiv 3 \pmod 4$, a contradiction.

Combining the two preceding propositions we see that the case $t = 4$ can occur only if $m = -1$.

Proposition 1.6. If $m \neq -3$, then 3 does not divide t, i.e. E has no $\mathbb{Q}$-rational points of order 3.

Proof: The proof follows the pattern of the two preceding proofs. Assume that $3 \mid t$. Then $3 \mid N_p$ for all $p \in \mathcal{P}$. If $p \in \mathcal{P}_1$, then $N_p = p + 1$ and $3 \nmid (p+1)$, so that $p \equiv -1 \pmod 3$. We now proceed to demonstrate the existence of a $p \in \mathcal{P}_1$ such that $p \equiv -1 \pmod 3$ in all cases where $m \neq -3$.

The case $m = -1$. There exist infinitely many primes in the arithmetic progression $12r + 7$. Let p be one such belonging to $\mathcal{P}$. Then $\left(\frac{m}{p}\right) = \left(\frac{-1}{p}\right) = -1$. Thus $p \in \mathcal{P}_1$. But $p \equiv 1 \pmod 3$, a contradiction.

The case $m = -2$. There exist infinitely many primes in the arithmetic progression $24r + 13$. Let p be one such belonging to $\mathcal{P}$. Then $\left(\frac{m}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{2}{p}\right) = -1$. Thus $p \in \mathcal{P}_1$. But $p \equiv 1 \pmod 3$, a contradiction.

The case $m = -11$. There exist infinitely many primes in the arithmetic progression $132r + 109$. Let p be one such belonging to $\mathcal{P}$.

Then $\left(\frac{m}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{11}{p}\right) = \left(\frac{p}{11}\right) = \left(\frac{-1}{11}\right) = -1$. Thus $p \in \mathcal{P}_1$. But $p \equiv 1 \pmod 3$, a contradiction.

The case $m = -7, -19, -43, -67, -163$. Notice that all of these satisfy $-m \equiv 7 \pmod{12}$. There exist infinitely many primes in the arithmetic progression $(-12m)r - (2m+1)$. Let p be one such belonging to $\mathcal{P}$. Then $\left(\frac{m}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-m}{p}\right) = \left(\frac{p}{-m}\right) = \left(\frac{-1}{-m}\right) = -1$. Thus $p \in \mathcal{P}_1$. But $p \equiv 1 \pmod 3$, a contradiction.

§2.) The case $j = 0$, $m = -3$, $f = 1$, and $Y^2 = X^3 + a_6$

In this section we examine the case $j = 0$ and give necessary and sufficient conditions on a_6 in order that t take on the values 1,2,3, or 6. As a corollary we obtain easily a classical result due to Fueter [1]. In addition, we derive formulas concerning $\mathbb{Q}$-rational points of order 3 on E which will be of use to us later.

Let E be any elliptic curve defined over $\mathbb{Q}$. E is isomorphic over $\mathbb{Q}$ to an elliptic curve given by an affine equation of the form

$$Y^2 = X^3 + a_4X + a_6 \tag{2.1}$$

with $a_4, a_6 \in \mathbb{Z}$.

The $\mathbb{Q}$-rational points of order 2 on (2.1) are of the form $(x,0)$ where x is a root of $X^3 + a_4X + a_6$.

Suppose now that $P = (x,y)$ is a $\mathbb{Q}$-rational point of order 3 on E, i.e. $2P = -P$. Then $y \neq 0$. Let

$$\lambda = (3x^2+a_4)/2y \tag{2.2}$$ and

$$\nu = y - \lambda x \tag{2.3}$$

By the usual formula for the addition of points on E, we have $2P = (\lambda^2-2x,-\lambda^3+3\lambda x-y)$. A $\mathbb{Q}$-rational point $P = (x,y)$ on E is a point of order $3 \iff (\lambda^2-2x,-\lambda^3+3\lambda x-y) = 2P = -P = (x,-y)$. This gives the necessary condition

$$\lambda^2 - 2x = x \qquad \text{or} \tag{2.4}$$

$$12xy^2 = 9x^4 + 6a_4x^2 + a_4^2 \tag{2.5}$$

Since $P = (x,y)$ lies on the curve, we have

$$12xy^2 = 12x^4 + 12a_4x^2 + 12a_6x \tag{2.6}$$

Subtract (2.5) from (2.6) and get

$$0 = 3x^4 + 6a_4x^2 + 12a_6x - a_4^2 \tag{2.7}$$

For the remainder of §2, we shall assume that $j = 0$. This is equivalent to assuming that $a_4 = 0$ by the formulas (1.2) applied to equation (2.1). Then (2.1) reduces to

$$Y^2 = X^3 + a_6 \,. \tag{2.8}$$

Such an elliptic curve E has complex multiplication in $\mathbb{Q}(\sqrt{-3})$ and $f = 1$.
By Proposition 1.4, $t \neq 4$. Thus $t = 1,2,3,$ or 6.

Proposition 2.1. E has a $\mathbb{Q}$-rational point of order $2 \iff a_6$ is a cube in $\mathbb{Z}$.

Proof: Points $(x,0)$ of order 2 on E correspond to roots of $X^3 + a_6$. One of these roots is in $\mathbb{Q} \iff -a_6$ is a cube in $\mathbb{Z}$ $\iff a_6$ is a cube in $\mathbb{Z}$.

If p is a prime, let v_p denote the usual p-adic valuation,

i.e. $v_p(p) = 1$.

Proposition 2.2. E has a $\mathbb{Q}$-rational point of order 3 $\Longleftrightarrow$ either a_6 is a square in $\mathbb{Z}$ or a_6 is equal to -432 times a sixth power in $\mathbb{Z}$.

Proof: Let $P = (x,y)$ be a $\mathbb{Q}$-rational point of order 3. Equation (2.7) reduces to $0 = 3x^4 + 12a_6x$. If $x = 0$, then $y^2 = a_6$, so that a_6 is a square in $\mathbb{Z}$. Conversely, this gives a $\mathbb{Q}$-rational point of order 3. If $x \neq 0$, then $0 = 3x^3 + 12a_6$ or $x^3 = -4a_6$. Thus $-4a_6$ must be a cube in $\mathbb{Z}$. $y^2 = x^3 + a_6 \Rightarrow y^2 = -4a_6 + a_6 = -3a_6 \Rightarrow -3a_6$ is a square in $\mathbb{Z}$. This implies that $v_2(a_6) \equiv 4 \pmod 6$, $v_3(a_6) \equiv 3 \pmod 6$, and $v_p(a_6) \equiv 0 \pmod 6$ for $p \geq 5$. Thus a_6 may be written as $a_6 = -2^4 3^3 t^6 = -432t^6$ for $t \in \mathbb{Z}$. Conversely this gives a $\mathbb{Q}$-rational point of order 3 on E.

Putting these results together, we have the following theorem.

Theorem 2.3. Let E be an elliptic cirve defined over $\mathbb{Q}$ with j-invariant $j = 0$ given by the affine equation $Y^2 = X^3 + a_6$ with $a_6 \in \mathbb{Z}$. Then

(1) $t = 6$ and $T(E) \cong \mathbb{Z}/6\mathbb{Z} \Longleftrightarrow a_6$ is a sixth power in $\mathbb{Z}$.

(2) $t = 3$ and $T(E) \cong \mathbb{Z}/3\mathbb{Z} \Longleftrightarrow$ either a_6 is a square in $\mathbb{Z}$ but not a sixth power in $\mathbb{Z}$ or a_6 is -432 times a sixth power.

(3) $t = 2$ and $T(E) \cong \mathbb{Z}/2\mathbb{Z} \Longleftrightarrow a_6$ is a cube in $\mathbb{Z}$ but not a sixth power in $\mathbb{Z}$.

(4) $t = 1$ and $T(E) = \{e\}$ otherwise.

An immediate corollary is the following classical result due to Fueter [1] (see also Mordell [3,4]).

Corollary 2.4. (Fueter) Let E be given by $Y^2 = X^3 + a_6$. Assume a_6 is sixth-powerfree. Let $P = (x,y)$ be a $\mathbb{Q}$-rational point on E such that $xy \neq 0$. Then P has infinite order unless $a_6 = 1$ and $P = (2,\pm 3)$ or $a_6 = -432$ and $P = (12,\pm 36)$.

§3) The case $j = 2^6 3^3$, $m = -1$, $f = 1$, and $Y^2 = X^3 + a_4 X$

Throughout this § we assume that $j = 2^6 3^3$. An elliptic curve E defined over $\mathbb{Q}$ with $j = 2^6 3^3$ is isomorphic over $\mathbb{Q}$ to an elliptic curve given by an affine equation of the form

$$Y^2 = X^3 + a_4 X \tag{3.1}$$

with $a_4 \in \mathbb{Z}$. The point $(0,0)$ is clearly a $\mathbb{Q}$-rational point of order 2 on E. By Proposition 1.6, t is either 2 or 4. The case $t = 4$ can occur either with the existence of 3 $\mathbb{Q}$-rational points of order 2 on E or with the existence of a $\mathbb{Q}$-rational point of order 4 on E.

Proposition 3.1. $t = 4$ and E has 3 $\mathbb{Q}$-rational points of order 2 $\Longleftrightarrow$ $-a_4$ is a square in $\mathbb{Z}$. In this case, $T(E) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Proof: A $\mathbb{Q}$-rational point $P = (x,y)$ on E has order 2 $\Longleftrightarrow y = 0$ and x is a solution of

$$0 = X^3 + a_4 X = X(X^2 + a_4) \tag{3.2}$$

Thus E has 3 $\mathbb{Q}$-rational points of order 2 $\Longleftrightarrow X^2 + a_4 = 0$ has

a solution in $\mathbb{Z}$ <==> $-a_4$ is a square in $\mathbb{Z}$.

Proposition 3.2. $t = 4$ and E has a $\mathbb{Q}$-rational point of order 4 <==> a_4 is equal to 4 times a fourth power in $\mathbb{Z}$. In this case $T(E) \cong \mathbb{Z}/4\mathbb{Z}$.

Proof: (==>) Let $P = (x,y)$ be a $\mathbb{Q}$-rational point of order 4 on E. Then $x \neq 0$, $y \neq 0$ and $2P = (0,0)$. Let $\lambda = (3x^2+a_4)/2y$. Using the usual formulas for the addition of points on an elliptic curve given by (3.1), we obtain $0 = \lambda^2 - 2x$ and $0 = y - \lambda x$. Thus $(3x^2+a_4)/2 = \lambda y = \lambda^2 x = 2x^2$ or $3x^2 + a_4 = 4x^2$ or $x^2 = a_4$. Thus $a_4 > 0$ and a_4 is a square in $\mathbb{Z}$. Since (x,y) lies on the curve E, $y^2 = x^3 + a_4x = x^3 + x^3 = 2x^3$. Thus $2|y$. Therefore $4|y^2$ and $4|2x^3$, so $2|x$ and $2|a_4$. a_4 is a square, so we may write $a_4 = (2b)^2$ with $b > 0$. Since $y^2 = x^3 + a_4x$ and $a_4 > 0$, we must have $x > 0$. $x^2 = a_4 = (2b)^2$, so that $x = 2b$. Then $y^2 = x^3 + a_4x = 2x^3 = 2(2b)^3 = 12b^3$. $2v_p(y/4) = 3v_p(b)$. Thus $v_p(b)$ is even for all p, i.e. b is a square. Write $b = c^2$ for $c \in \mathbb{Z}$. We have $a_4 = (2b)^2 = 4b^2 = 4c^4$.

(<==) Suppose $a_4 = 4c^4$ for $c \in \mathbb{Z}$. Let $x = 2c^2$, $y = 4c^3$. $P = (x,y)$ is a $\mathbb{Q}$-rational point on E of order 4.

Proposition 3.3. $t = 2$ <==> a_4 is neither of the form $a_4 = 4c^4$ for some $c \in \mathbb{Z}$ nor of the form $a_4 = -c^2$ for some $c \in \mathbb{Z}$. In this case, $T(E) \cong \mathbb{Z}/2\mathbb{Z}$.

§4.) The existence of points of order 2

Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant

$j \neq 0$. In this section we show that the existence of a $\mathbb{Q}$-rational point on E of order 2 is dependent only on the value of the j-invariant of E, i.e. if one elliptic curve E defined over $\mathbb{Q}$ has a $\mathbb{Q}$-rational point of order 2, then all other elliptic curves defined over $\mathbb{Q}$ with the same j-invariant have such a point. This is accomplished by setting up a standard form for an affine equation for E and seeing that the existence of a $\mathbb{Q}$-rational point of order 2 depends solely on the value of j. In particular, we set ourselves the task of showing that an elliptic curve E defined over $\mathbb{Q}$ always possesses a $\mathbb{Q}$-rational point of order 2 provided that the j-invariant of E takes on one of the following values:
$j = 2^6 3^3$, $2^6 5^3$, $-3^3 5^3$, $2^3 3^3 11^3$, $2^4 3^3 5^3$, and $3^3 5^3 17^3$.

E is always isomorphic over $\mathbb{Q}$ to an elliptic curve defined by an affine equation of the form

$$Y^2 = X^3 + a_4 X + a_6 \tag{4.1}$$

with $a_4, a_6 \in \mathbb{Z}$. Applying the formulas (1.2) to the equation (4.1), we obtain

$$\begin{aligned} b_2 &= 0 \\ b_4 &= 2a_4 \\ b_6 &= 2^2 a_6 \\ b_8 &= -a_4^2 \\ c_4 &= -2^4 3^1 a_4 \\ c_6 &= -2^5 3^3 a_6 \\ \Delta &= -2^4 (2^2 a_4^3 + 3^3 a_6^2) \\ j &= 2^8 3^3 a_4^3 / (2^2 a_4^3 + 3^3 a_6^2) \end{aligned} \tag{4.2}$$

We have

$$(4.3) \qquad 2^8 3^3 a_4^3 = j(2^2 a_4^3 + 3^3 a_6^2)$$

Notice that $j = 0 \iff a_4 = 0$ and that $j = 2^6 3^3 \iff a_6 = 0$. These cases have been discussed in §2 and §3; for the remainder of this § we assume that $j \neq 0$ and $j \neq 2^6 3^3$.

A $\mathbb{Q}$-rational point $P = (x,y)$ on the elliptic curve defined by (4.1) is of order $2 \iff y = 0$, $x \in \mathbb{Z}$, and

$$(4.4) \qquad 0 = x^3 + a_4 x + a_6$$

Thus we seek integer solutions to the equation

$$(4.5) \qquad 0 = X^3 + a_4 X + a_6$$

Notice that x is a root of $X^3 + a_4 X + a_6 \iff -x$ is a root of $X^3 + a_4 X - a_6$. We may therefore assume $a_6 > 0$. Rewrite (4.3) as

$$(4.6) \qquad (2^8 3^3 - 2^2 j) a_4^3 = 3^3 j\, a_6^2$$

Clearly $a_4 > 0 \iff 3^3 j / (2^8 3^3 - 2^2 j) > 0$. Let $\epsilon = a_4/|a_4|$. Let $s_p = v_p(3^3 j) - v_p(2^8 3^3 - 2^2 j) = v_p(3^3 j/(2^8 3^3 - 2^2 j))$. Let $S = \{p \mid s_p \neq 0\}$. ϵ and S depend only on j and not on a_4 and a_6. Applying v_p to (4.6), we have

$$(4.7) \qquad 3v_p(a_4) = 2v_p(a_6) + s_p$$

Let $r_p = (v_p(a_4) - |s_p|)/2$. By (4.7) this is an integer. Let $D = \prod_p p^{r_p}$. Then $v_p(a_4) = 2r_p + |s_p|$, so that $a_4 = \epsilon(\prod_{p \in S} p^{|s_p|}) D^2 = A D^2$ for $A = \epsilon \prod_{p \in S} p^{|s_p|}$. Similarly $v_p(a_6) - 3r_p = v_p(a_6) - (3v_p(a_4) - 3|s_p|)/2 = (2v_p(a_6) - 3v_p(a_4) + 3|s_p|)/2 = (-s_p + 3|s_p|)/2$. Thus $v_p(a_6) - 3r_p = s_p$ if $s_p \geq 0$ and $v_p(a_6) - 3r_p = -2s_p$ if $s_p < 0$. Let $B = (\prod_{\substack{p \in S \\ s_p > 0}} p^{s_p})(\prod_{\substack{p \in S \\ s_p < 0}} p^{-2s_p})$. Then $a_6 = B D^3$

since we assumed $a_6 > 0$.

A and B depend only on j and not on a_4 and a_6. Equation (4.5) may be written as

$$(4.8) \qquad 0 = X^3 + A D^2 X + B D^3$$

Let $X = DW$. Substituting in (4.8), we obtain

$$(4.9) \qquad 0 = D^3W^3 + A D^3W + B D^3 \qquad \text{or}$$

$$(4.10) \qquad 0 = W^3 + AW + B$$

The solutions to (4.8) correspond to the solutions to (4.10) via $X = DW$. Equation (4.10) depends only on j. We have thus proved the following theorem.

Theorem 4.1. Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant $j \neq 0, 2^6 3^3$. E has a $\mathbb{Q}$-rational point of order 2 $\Longleftrightarrow$ there exists an integer solution to equation (4.10). E has 3 $\mathbb{Q}$-rational points of order 2 $\Longleftrightarrow$ there exist 3 integer solutions to equation (4.10). This depends only on j.

We can now apply this result to the values of j listed at the outset of this section. The procedure in each case is to find equation (4.10) and then check this for integer solutions.

Corollary 4.2. Let E be an elliptic curve defined over $\mathbb{Q}$ whose j-invariant takes on one of the following values: $j = 2^6 3^3, 2^6 5^3, -3^3 5^3, 2^3 3^3 11^3, 2^4 3^3 5^3$, and $3^3 5^3 17^3$. Then E has at least one $\mathbb{Q}$-rational point of order 2.

Proof: The case $j = 2^6 3^3$. This has been discussed in § 3.

The case $j = 2^6 5^3$. $3^3 j/(2^8 3^3 - 2^2 j) = -2^{-3} 3^3 5^3 7^{-2}$, $\epsilon = -1$, $S = \{2,3,5,7\}$, $s_2 = -3$, $s_3 = 3$, $s_5 = 3$, $s_7 = -2$. Thus $A = -2^3 3^3 5^3 7^2$ and $B = 2^6 3^3 5^3 7^4$. Equation (4.10) becomes $0 = W^3 - 2^3 3^3 5^3 7^2 W + 2^6 3^3 5^3 7^4$. This has the solution $W = 2^3 3^1 5^1 7^1$.

The case $j = -3^3 5^3$. Equation (4.10) becomes $0 = W^3 - 2^2 5^3 7^1 W + 2^4 5^3 7^2$. This has the solution $W = -2^1 5^1 7^1$.

The case $j = 2^3 3^3 11^3$. Equation (4.10) becomes $0 = W^3 - 2^2 7^2 11^3 W + 2^4 7^4 11^3$ and $W = 2^2 7^1 11^1$ is a solution.

The case $j = 2^4 3^3 5^3$. Equation (4.10) becomes $0 = W^3 - 2^2 3^3 5^3 11^2 W + 2^4 3^3 5^3 11^4$ and $W = 2^2 3^1 5^1 11^1$ is a solution.

The case $j = 3^3 5^3 17^3$. Equation (4.10) becomes $0 = W^3 - 2^2 3^2 5^3 7^1 17^3 19^2 W + 2^4 3^4 5^3 7^2 17^3 19^4$ and $W = 2^2 3^1 5^1 7^1 17^1 19^1$ is a solution.

Corollary 4.3. Let E be an elliptic curve defined over $\mathbb{Q}$ whose j-invariant is $j = 2^3 3^3 11^3$. Then E possesses only one $\mathbb{Q}$-rational point of order 2.

Proof: Equation (4.10) becomes $0 = W^3 - 2^2 7^2 11^3 W + 2^4 7^4 11^3$. Let $W = 2^1 7^1 11^1 Z$. Solving (4.10) is equivalent to solving $0 = Z^3 - 11Z + 14$. The only rational solution to the latter is $Z = 2$.

We could continue to examine some of the other values of j corresponding to elliptic curves with complex multiplication and show that they did not have any $\mathbb{Q}$-rational points of order 2 by the methods of Theorem 4.1. However, we will develop a slightly different technique in the next section which will provide us with these results.

§ 5.) Some necessary conditions for the existence of $\mathbb{Q}$-rational points of order 2.

Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant $j \neq 0$. In this section we establish certain necessary conditions on the j-invariant for E to have a $\mathbb{Q}$-rational point of order 2. As a corollary we are able to conclude easily that elliptic curves defined over $\mathbb{Q}$ with the following j-invariants possess no non-trivial $\mathbb{Q}$-rational points of finite order: $j = -2^{15}$, $-2^{15}3^3$, $-2^{18}3^35^3$, $-2^{15}3^35^311^3$, or $-2^{18}3^35^323^329^3$.

E is isomorphic over $\mathbb{Q}$ to an elliptic curve defined by an affine equation of the form

$$Y^2 = X^3 + a_4'X + a_6' \tag{5.1}$$

with $a_4', a_6' \in \mathbb{Z}$. Suppose now that E has a $\mathbb{Q}$-rational point $P = (x,y)$ of order 2. Then $y = 0$ and $x \in \mathbb{Z}$. By translation $(X \mapsto X + x,\ Y \mapsto Y)$, we obtain an elliptic curve isomorphic over $\mathbb{Q}$ to E given by an affine equation of the form

$$Y^2 = X^3 + a_2X^2 + a_4X \tag{5.2}$$

with $a_2, a_4 \in \mathbb{Z}$. Applying formulas (1.2) to (5.2), we see that

$$\begin{aligned} b_2 &= 2^2a_2 \\ b_4 &= 2a_4 \\ b_6 &= 0 \\ b_8 &= -a_4^2 \\ c_4 &= 2^4(a_2^2 - 3a_4) \\ c_6 &= -2^6a_2^3 - 2^53^2a_2a_4 \\ \Delta &= 2^4(a_2^2a_4^2 - 2^2a_4^3) \\ j &= 2^8(a_2^2 - 3a_4)^3/(a_2^2a_4^2 - 2^2a_4^3) \end{aligned} \tag{5.3}$$

Let $g = a_2^2 - 3a_4$. Then

$$(5.4) \qquad j = 2^8 g^3 / a_4^2 (g - a_4)$$

for an elliptic curve given by (5.2).

Proposition 5.1. Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant $j \neq 0$. Assume that E has a $\mathbb{Q}$-rational point of order 2. Then the following holds:

(1) If $v_2(j) > 8$, then $3 | (v_2(j) - 8)$.

(2) If $v_p(j) > 0$ for a prime $p \geq 3$, then $3 | v_p(j)$.

Proof: E is isomorphic over $\mathbb{Q}$ to an elliptic curve given by an affine equation of the form (5.2). Let $d_2 = v_2(j) - 8$ and $d_p = v_p(j)$ for $p \geq 3$. The assumption in (1) and (2) may then be phrased uniformly as $d_p > 0$.
Apply v_p to equation (5.4) and obtain $d_p = 3v_p(g) - 2v_p(a_4) - v_p(g - a_4)$. If $v_p(g) \leq v_p(a_4)$, then $v_p(g - a_4) \geq v_p(g)$ and $d_p \leq 0$, a contradiction. Thus $v_p(g) > v_p(a_4)$ and $v_p(g - a_4) = v_p(a_4)$. We obtain $d_p = 3[v_p(g) - v_p(a_4)]$. Thus $3 | d_p$.

Corollary 5.2. Let E be an elliptic curve defined over $\mathbb{Q}$ whose j-invariant takes on one of the following values: $j = -2^{15}$, $-2^{15}3^3$, $-2^{18}3^35^3$, $-2^{15}3^35^311^3$, $-2^{18}3^35^323^329^3$. Then E does not have any non-trivial $\mathbb{Q}$-rational points of finite order, i.e. $t = 1$ and $T(E) = \{e\}$.

Proof: In all these cases $v_2(j) > 8$ and 3 does not divide $v_2(j) - 8$. By Proposition 5.1, E cannot have a $\mathbb{Q}$-rational point of order 2. E admits complex multiplication in $\mathbb{Q}(\sqrt{m})$ for $m \neq -3$ for the values of j listed above. By Proposition 1.6, E has no

$\mathbb{Q}$-rational point of order 3. Proposition 1.3 concludes the proof.

Corollary 5.3. Let E be an elliptic curve defined over $\mathbb{Q}$ whose j-invariant is $j = -2^{15}3^{1}5^{3}$. E does not have a $\mathbb{Q}$-rational point of order 2.

Proof: Apply Proposition 5.1.

Remark. That $v_2(j) > 8$ is a necessary assumption in Proposition 5.1 may be seen by examining the curve $Y^2 = X^3 + X$. This curve certainly has a $\mathbb{Q}$-rational point of order 2, namely $(0,0)$. $j = 2^6 3^3$, so that 3 does not divide $v_2(j) - 8$.

§6.) $\mathbb{Q}$-rational points of order 4.

In this section we give necessary and sufficient conditions for an elliptic curve E defined over $\mathbb{Q}$ with j-invariant $j = 2^3 3^3 11^3$ to have a $\mathbb{Q}$-rational point of order 4.

By the results of §4, E is isomorphic over $\mathbb{Q}$ to an elliptic curve given by an affine equation of the form

$$(6.1) \qquad Y^2 = X^3 + AD^2X + BD^3$$

where $A = -2^2 7^2 11^3$, $B = 2^4 7^4 11^3$, and $D \in \mathbb{Z}$, $D \neq 0$. By Corollary 4.3, this curve has exactly one $\mathbb{Q}$-rational point of order 2.

Let $a = 2^2 7^1 11^1 D$. The point $(a,0)$ is the $\mathbb{Q}$-rational point of order 2 on E. By the translation $X \mapsto X + a$, $Y \mapsto Y$ employed in §5, the following equation is obtained:

$$(6.2) \qquad Y^2 = X^3 + a_2X^2 + a_4X$$

where $a_2 = 2^2 3^1 7^1 11^1 D$ and $a_4 = 2^2 7^2 11^2 D^2$.

Theorem 6.1. Let E be an elliptic curve defined over $\mathbb{Q}$ with j-invariant $j = 2^3 3^3 11^3$ given by (6.2). E has a $\mathbb{Q}$-rational point of order $4 \iff v_7(D)$ and $v_{11}(D)$ are odd and $v_p(D)$ is even for $p \geq 3$ with $p \neq 7, 11$. In this case, $t = 4$ and $T(E) \cong \mathbb{Z}/4\mathbb{Z}$. Otherwise $t = 2$ and $T(E) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof: By Proposition 1.6, E has no $\mathbb{Q}$-rational points of order 3. By Corollary 4.3 it has only one $\mathbb{Q}$-rational point of order 2. Proposition 1.3 then implies that $t = 2$ or 4 (cyclic). We are thus reduced to investigating the existence of a $\mathbb{Q}$-rational point of order 4 on E. The point $(0,0)$ is the only $\mathbb{Q}$-rational point of order 2 on (6.2).

Suppose that $P = (x,y)$ is to be a $\mathbb{Q}$-rational point of order 4. Then $2P = (0,0)$. Let $\lambda = (3x^2+2a_2x+a_4)/2y$ and $\nu = y - \lambda x$. Then

$$2\lambda y = 3x^2 + 2a_2x + a_4 \tag{6.3}$$

By the formula for the addition of points on E, we must have

$$0 = \lambda^2 - a_2 - 2x \tag{6.4}$$

and

$$0 = \nu \ . \tag{6.5}$$

Thus

$$y = \lambda x \quad \text{or} \quad \lambda = y/x \ . \tag{6.6}$$

Substituting (6.6) in (6.3), we obtain

$$2y^2 = 3x^3 + 2a_2x^2 + a_4x \tag{6.7}$$

Since (x,y) is to be a point on (6.2), we should have $2y^2 = 2x^3 + 2a_4x^2 + 2a_2x$.

Subtracting this from (6.7) gives

$$(6.8) \qquad 0 = x^3 - a_4 x$$

Now $x = 0$ is not possible if (x,y) is to have order 4. Thus

$$(6.9) \qquad x^2 - a_4 = 0 .$$

Since $a_4 = 2^2 7^2 11^2 D^2$, then $x = \sigma 2^1 7^1 11^1 D$ where $\sigma = \pm 1$. Substituting in (6.2), we have

$$\begin{aligned} y^2 &= \sigma^3 2^3 7^3 11^3 D^3 + 2^4 3^1 7^3 11^3 D^3 + \sigma 2^3 7^3 11^3 D^3 \\ &= 2^3 7^3 11^3 D^3 \, (\sigma + 6 + \sigma) \\ &= \begin{cases} 2^6 7^3 11^3 D^3 & \text{if } \sigma = 1 \\ 2^5 7^3 11^3 D^3 & \text{if } \sigma = -1 \end{cases} \end{aligned} \tag{6.10}$$

If $v_2(D)$ is even, let $\sigma = 1$; if $v_2(D)$ is odd, let $\sigma = -1$. Applying v_p to (6.10), we see that there exists a $y \in \mathbb{Z}$ satisfying (6.10) $\iff$ $v_p(D)$ satisfies the conditions stated in the theorem.

§7.) $\mathbb{Q}$-rational points of order 3

There are two j-invariants remaining which allow for the possibility of the existence of a $\mathbb{Q}$-rational point of order 3, namely $j = 2^4 3^3 5^3$ and $j = -2^{15} 3^1 5^3$. In this section necessary and sufficient conditions are given for such points to exist.

Assume that the elliptic curve E is given by an affine equation of the form

$$(7.1) \qquad Y^2 = X^3 + a_4 X + a_6$$

with $a_4, a_6 \in \mathbb{Z}$. Suppose that $P = (x,y)$ is a $\mathbb{Q}$-rational point

of order 3 on E. Recall from §2 that a necessary condition on P is

$$(7.2) \qquad 0 = 3x^4 + 6a_4x^2 + 12a_6x - a_4^2 .$$

Theorem 7.1. Let E be an elliptic curve defined over $\mathbb{Q}$ with $j = -2^{15}3^1 5^3$. We may assume that E is given by (7.1) where $a_4 = -2^7 3^3 5^3 11^2 23^2 D^2$ and $a_6 = 2^7 3^3 5^3 11^4 23^4 D^3$ for $D \in \mathbb{Z}$. E has a $\mathbb{Q}$-rational point of order 3 $\iff$ $v_p(D)$ is odd for $p = 2,3,5,11,23$ and $v_p(D)$ is even for all other primes p. In this case, $t = 3$ and $T(E) \cong \mathbb{Z}/3\mathbb{Z}$. Otherwise $t = 1$ and $T(E) = \{e\}$.

Proof: Proposition 1.3 and Corollary 5.3 imply that t is either 1 or 3. We apply the techniques of §4 to E. In the notation of §4, $3^3 j/(2^8 3^3 - 2^2 j) = -2^7 3^3 5^3 11^{-2} 23^{-2}$, $\epsilon = -1$, $A = -2^7 3^3 5^3 11^2 23^2$, $B = 2^7 3^3 5^3 11^4 23^4$, $a_4 = AD^2$, and $a_6 = BD^3$. Thus we may assume that E is given by the affine equation indicated above. Suppose $P = (x,y)$ is to be a $\mathbb{Q}$-rational point of order 3. Substituting in (7.2) we obtain

$$(7.3) \qquad 0 = 3x^4 - 2^8 3^4 5^3 11^2 23^2 D^2 x^2 + 2^9 3^4 5^3 11^4 23^4 D^3 x - 2^{14} 3^6 5^6 11^4 23^4 D^4$$

Let $x = 2^3 3^1 5^1 11^1 23^1 Dz$. (7.3) then reduces to

$$(7.4) \qquad 0 = z^4 - 60z^2 + 253z - 300$$

One checks that $z = 3$ is the only integer solution. Thus $x = 2^3 3^2 5^1 11^1 23^1 D$. If $P = (x,y)$ is to lie on E, then

$$(7.5) \qquad y^2 = x^3 + a_4x + a_6 \qquad \text{or}$$

$$(7.6) \qquad y^2 = 2^7 3^3 5^3 11^3 23^3 D^3$$

Hence $y \in \mathbb{Z} \iff v_p(D)$ is odd for $p = 2,3,5,11,23$ and $v_p(D)$ is even for all other primes p. Conversely such a point (x,y) gives a $\mathbb{Q}$-rational point of order 3 on E.

Theorem 7.2. Let E be an elliptic curve defined over $\mathbb{Q}$ with $j = 2^4 3^3 5^3$. We may assume E is given by (7.1) where $a_4 = -2^2 3^3 5^3 11^2 D^2$ and $a_6 = 2^4 3^3 5^3 11^4 D^3$ for $D \in \mathbb{Z}$. E has a $\mathbb{Q}$-rational point of order $3 \iff v_p(D)$ is odd for $p = 2,3,5,11$ and $v_p(D)$ is even for all other primes p. In this case, $t = 6$ and $T(E) \cong \mathbb{Z}/6\mathbb{Z}$. Otherwise $t = 2$ and $T(E) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof: Proposition 1.3, Proposition 1.4, and Corollary 4.2 imply that t is either 2 or 6. As in the preceding proof, we apply the techniques of §4 to obtain $A = -2^2 3^3 5^3 11^2$ and $B = 2^4 3^3 5^3 11^4$, so that E may be assumed to be given by the affine equation indicated above. (7.2) gives

$$(7.7) \qquad 0 = 3x^4 - 2^2 3^4 5^3 11^2 D^2 x^2 + 2^6 3^4 5^3 11^4 D^3 x - 2^4 3^6 5^6 11^4 D^4 .$$

Let $x = 2^1 3^1 5^1 11^1 Dz$. Substitute in (7.7) and reduce to

$$(7.8) \qquad 0 = z^4 - 30z^2 + 88z - 75 .$$

One checks that $z = 3$ is the only integer solution. $x = 2^1 3^2 5^1 11^1 D$. If $P = (x,y)$ is to lie on E, then

$$(7.9) \qquad y^2 = x^3 + a_4 x + a_6 \qquad \text{or}$$

$$(7.10) \qquad y^2 = 2^5 3^3 5^3 11^3 D^3 .$$

Hence $y \in \mathbb{Z} \iff v_p(D)$ is odd for $p = 2,3,5,11$ and $v_p(D)$ is even for all other primes p. Conversely such a point (x,y) gives

a $\mathbb{Q}$-rational point of order 3 on E.

This completes the determination of T(E) for all elliptic curves E defined over $\mathbb{Q}$ admitting complex multiplication. The results are summarized in the accompanying table.

§8.) Anomalous primes

One of the original motivations for undertaking the investigation carried out here was to search for an explanation for various phenomena which occur in connection with the theory of anomalous primes. Let E be an elliptic curve defined over $\mathbb{Q}$ and let p be a prime where E has good reduction. We say that p is <u>anomalous for E</u> if $f_p = 1 + p - N_p$ (with the notation of §1) is congruent to 1 modulo p, i.e. if $N_p \equiv 0 \pmod{p}$. Let Anom(E) denote the set of all such. Mazur [2] has shown the importance of such primes in the study of the group of rational points on E in towers of number fields. One of his results is that Anom(E) has at most 3 elements (easily computable) if E possesses non-trivial $\mathbb{Q}$-rational points of finite order. In an investigation of anomalous primes for elliptic curves with complex multiplication, Olson [5] showed that Anom(E) has at most 1 element (equal to 2,3, or 5) if m = -1,-2, or -7 and if f = 2, then Anom(E) is empty. A natural question which then arises in this context is whether this latter result could be related to the existence of non-trivial $\mathbb{Q}$-rational points of finite order on E. A glance at the accompanying table reveals that this is indeed the case.

Bibliography

1.) Fueter, R. Über kubische diophantische Gleichungen, Commentarii Math. Helv., 2 (1930), 69-89.

2.) Mazur, B. Rational points of abelian varieties with values in towers of number fields, Invent. Math. 18 (1972), 183-266.

3.) Mordell, L.J. Diophantine Equations. Academic Press, London, 1969.

4.) Mordell, L.J. The infinity of rational solutions of $y^2 = x^3+k$, J. Lond. Math. Soc., 41 (1966), 523-525.

5.) Olson, L.D. Hasse invariants and anomalous primes for elliptic curves with complex multiplication, to appear in J. of Number Theory.

6.) Serre, J.P. Complex multiplication in J.W.S. Cassels and A. Fröhlich, Algebraic Number Theory, Thompson Book Company, Washington, D.C., U.S.A., 1967.

7.) Serre, J.P. Groupes de Lie l-adiques attachés aux courbes elliptiques, Coll. Internat. du C.N.R.S., No. 143 a Clermont-Ferrand, Editions du C.N.R.S., Paris, 1966.

8.) Tate, J. The arithmetic of elliptic curves. Colloquium Lectures given at Dartmouth College, August 29 - September 1, 1972.